S

ENGINEERING CHANGE NOTICE

Page 1 of 2

1. ECN 600250

Proj. ECN

2. ECN Category (mark one)	3. Originator's Name, Organization, MSIN, and Telephone No.	4. USQ Required?	5. Date
Supplemental ☒	J.B ROBERTS/SST ENGR/T4-07/373-7912	☒ Yes ☐ No	2/14/01
Direct Revision ☒			
Change ECN ☐			
Temporary ☐			
Standby ☐			
Supersedure ☐			
Cancel/Void ☐			

6. Project Title/No./Work Order No.	7. Bldg./Sys./Fac. No.	8. Approval Designator
CROSS-SITE LOG BOOK	242-S	N/A
9. Document Numbers Changed by this ECN (includes sheet no. and rev.)	**10. Related ECN No(s).**	**11. Related PO No.**
HNF-2544 , Rev. 0	N/A	N/A

12a. Modification Work	12b. Work Package No.	12c. Modification Work Completed	12d. Restored to Original Condition (Temp. or Standby ECNs only)
☐ Yes (fill out Blk. 12b) ☒ No (NA Blks. 12b, 12c, 12d)	N/A	N/A Design Authority/Cog. Engineer Signature & Date	N/A Design Authority/Cog. Engineer Signature & Date

13a. Description of Change

13b. Design Baseline Document? ☒ Yes ☐ No

Replace Rev. 0 of HNF-2544 with Rev. 1

USQ TF-01-0122, Rev. 0

14a. Justification (mark one)	
Criteria Change	☐
Design Improvement	☒
Environmental	☐
Facility Deactivation	☐
As-Found	☐
Facilitate Const.	☐
Const. Error/Omission	☐
Design Error/Omission	☐

14b. Justification Details

This ECN updates the "Software Configuration Plan For The Replacement Cross-Site Transfer System Control System. The requirement to control the logbook per HNF-IP-0842, Vol. II, Operations, Section4.11.1, Operating Logbooks has been added.
The design verification is by informal review per IP-0842, Vol. IV, Section 4.24
This design change will not result in any radiation exposure increase.

15. Distribution (include name, MSIN, and no. of copies)

W.E. Bryan	T4-07
M.H. Brown	T4-07
J.B. Roberts	T4-07
T.G. Frater	T4-08
K.J. Anderson	T4-07

RELEASE STAMP

APR 12 2001

DATE:

STA: 5

HANFORD RELEASE

ID: 12

ENGINEERING CHANGE NOTICE

4/11/01
02
Page 2 of 4

1. ECN (use no. from pg. 1): ECN-600250

16. Design Verification Required	17. Cost Impact		18. Schedule Impact (days)
	ENGINEERING	CONSTRUCTION	
☒ Yes	Additional ☐ $ N/A	Additional ☐ $ N/A	Improvement ☐ N/A
☐ No	Savings ☐ $ N/A	Savings ☐ $ N/A	Delay ☐ N/A

19. Change Impact Review: Indicate the related documents (other than the engineering documents identified on Side 1) that will be affected by the change described in Block 13. Enter the affected document number in Block 20.

SDD/DD	☐	Seismic/Stress Analysis	☐	Tank Calibration Manual	☐
Functional Design Criteria	☐	Stress/Design Report	☐	Health Physics Procedure	☐
Operating Specification	☐	Interface Control Drawing	☐	Spares Multiple Unit Listing	☐
Criticality Specification	☐	Calibration Procedure	☐	Test Procedures/Specification	☐
Conceptual Design Report	☐	Installation Procedure	☐	Component Index	☐
Equipment Spec.	☐	Maintenance Procedure	☐	ASME Coded Item	☐
Const. Spec.	☐	Engineering Procedure	☐	Human Factor Consideration	☐
Procurement Spec.	☐	Operating Instruction	☐	Computer Software	☐
Vendor Information	☐	Operating Procedure	☐	Electric Circuit Schedule	☐
OM Manual	☐	Operational Safety Requirement	☐	ICRS Procedure	☐
FSAR/SAR	☐	IEFD Drawing	☐	Process Control Manual/Plan	☐
Safety Equipment List	☐	Cell Arrangement Drawing	☐	Process Flow Chart	☐
Radiation Work Permit	☐	Essential Material Specification	☐	Purchase Requisition	☐
Environmental Impact Statement	☐	Fac. Proc. Samp. Schedule	☐	Tickler File	☐
Environmental Report	☐	Inspection Plan	☐	NONE	☒
Environmental Permit	☐	Inventory Adjustment Request	☐		☐

20. Other Affected Documents: (NOTE: Documents listed below will not be revised by this ECN.) Signatures below indicate that the signing organization has been notified of other affected documents listed below.

Document Number/Revision	Document Number/Revision	Document Number/Revision
N/A	N/A	N/A

21. Approvals

	Signature	Date		Signature	Date
Design Authority JB ROBERTS	J B Roberts	2/14/01	Design Agent		
Cog. Eng. JB ROBERTS	J B Roberts	2/14/01	PE		
Cog. Mgr. WE BRYAN	W. E. Bryan	4/11/01	QA		
QA			Safety		
Safety			Design		
Environ.			Environ.		
Other			Other		
INF. REV. JA BEWICK	J A. Bewick	4/11/01			

DEPARTMENT OF ENERGY

Signature or a Control Number that tracks the Approval Signature

ADDITIONAL

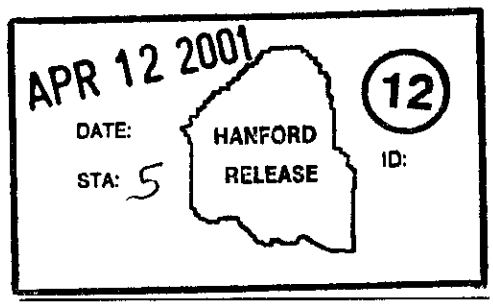
SOFTWARE CONFIGURATION PLAN FOR THE REPLACEMENT CROSS-SITE TRANSFER SYSTEM CONTROL SYSTEM

J.B. ROBERTS
CH2M HILL HANFORD GROUP
Richland, WA 99352
U.S. Department of Energy Contract DE-AC06-96RL13200

EDT/ECN: ECN-600250 UC:
Org Code: CL143200 Charge Code: 102523
B&R Code: Total Pages: 9

Key Words: Software Configuration Control Plan, Operating Control Station, OCS, Process Monitoring and Control System, W-058 Project, Replacement Cross-Site Transfer System, Allen-Bradley, RSI, SSTE.

Abstract: This document describes the formal documentation for maintaining the control system associated with the Replacement Cross-Site Transfer System. All Aspects of sofware quality assurance requirements are described here within.



Release Approval 4/12/01 Date

Release Stamp

Approved For Public Release

RECORD OF REVISION

(1) Document Number: HNF-2544

(2) Title: SOFTWARE CONFIGURATION PLAN FOR THE REPLACEMENT CROSS-SITE TRANSFER SYSTEM CONTROL SYSTEM

Change Control Record

(3) Revision	(4) Description of Change - Replace, Add, and Delete Pages	Authorized for Release	
		(5) Cog. Engr.	(6) Cog. Mgr. Date
0	(7) ORIGINAL RELEASE BY ETD-606480 dated 4/3/98	RE LARSON	RE LARSON 4/3/98
RS 1	LOGBOOK MAINTENANCE TO BE PER HNF-IP-0842, OPERATIONS, VOL. II, SECT. 4.11.1 PER ECN-600250	JB ROBERTS JB Roberts	WE BRYAN 4/12/01 W.E. Bryan 4/12/01

SOFTWARE CONFIGURATION PLAN FOR THE REPLACEMENT CROSS-SITE TRANSFER SYSTEM CONTROL SYSTEM

Prepared by
Jay B. Roberts
Single-Shell Tank Cog Engineering

February 15, 2001
CH2M Hill Hanford Group
Richland, Washington

CONTENTS

1.0 SOFTWARE CONFIGURATION CONTROL

1.1 INTRODUCTION

The objective of the software configuration control plan is to provide assurances that the replacement cross-site transfer system control system will be operable for the lifetime of the facility. To remain operable the control system shall be maintained by engineering (Single-Shell Tank Engineering [SSTE] personnel. Maintenance contract(s) with the software vendor shall be established to ensure the latest version of software is maintained on the control system. The computer operating system provides control of all cross-site equipment and is used for normal plant operations. Safety shutdowns of the transfer system are performed by hardwire components.

1.2 SCOPE

This plan covers the following topics: personnel authorized to make changes to the ladder logic, the methods, procedures and instructions used to control the identification of, access to, changes to, and the status of computer software. Configuration control documentation shall identify the changes to the ladder logic and work packages (e.g., test plans) shall be used to verify and validate the changes.

The software used on the control system is vendor supplied. All validation and verification shall be accomplished by the vendor (or the vendor's representative) and supplied to engineering (SSTE), as requested, prior to the use of updated software. No changes to the vendor-supplied software shall be done by engineering and/or any other contractors. The source code was not supplied, nor is it required, for the vendor supplied software.

1.3 PROJECT SCOPE

The design was based upon the criteria documented in the W-058 Project Procurement Specification (W-058-P2) for the "Process Monitor and Control System." A supplier, using the Allen-Bradley hardware and software, and the Fluor Daniel Northwest design media for Project W-058, procured hardware and software. After programming the ladder logic, the supplier assisted in installing and testing the equipment on-site. If required, a contract may be issued to the supplier for either software or hardware assistance.

The control console (located in the 242-S building) has two Pentium personal computers (an operator's station and a maintenance station). The control console software (Rockwell Software Incorporated [RSI]) interfaces with the Allen-Bradley PLC-5 programmable logic controllers. The control console is totally isolated from all other site computer systems.

The RSI software is being transferred into CH2M Hill Hanford Group's name. The engineering Point-of-Contact (PIC) is identified as the Monitor and Control Cog Engineer (SSTE), currently Jay B. Roberts (otherwise known as the Software Custodian).

2.0 SOFTWARE QUALITY ASSURANCE REQUIREMENTS

2.1 PERSONNEL AUTHORIZED TO MAKE CHANGES

The only personnel allowed to make changes to the ladder logic (not changes to the vendor supplied software) are members of the engineering organization (SSTE). Only members of engineering (SSTE) that have been trained on the Allen-Bradley software shall be allowed to make changes. These individuals shall have the "System Administrator" access to the ladder logic and vendor supplied software. The password to be used to enter the ladder logic level of the program shall be held by these individuals and a copy of all passwords shall be supplied to the Operations (Single-Shell Tanks [SST]) Manager. Nominally two engineers and the Engineering (SSTE) Manager shall be permitted to access the ladder logic.

A minimum of two engineering personnel shall be capable of working with the control station. The engineering personnel shall be capable of forcing functions (inputs and outputs) from the control console, as required for testing. All forcing functions and any identified control system problems shall be documented in the W-058 Control System Logbook. The logbook is located in the W-058 control room (242-S building) and will only be removed (for short periods) when copies of logbook pages are needed. The logbook shall be maintained in accordance with HNF-IP-0842, *Operations,* Volume II, Section 4.11.1, "Operating Logbooks."

2.2 METHODS, PROCEDURES, INSTRUCTIONS AND STATUS

This document defines the control methodology to be used to maintain the ladder logic configuration.

2.2.1 METHODS

The ladder logic is identified in document HNBF-2346, "Project W-058 Monitor and Control System Logic." The ladder logic shall be maintained by using the current supporting document change control process (Engineering Change Notices [ECN]).

All permanent changes to ladder logic shall go through the formal change control (ENC) process. The level of the change to the ladder logic shall determine the level of independent overview organization (QA and Safety) reviews required. The changes, when incorporated into the computer ladder logic, shall be recorded in the W-058 Control System Logbook.

2.2.2 PROCEDURES

The individual starting up either of the computers is required to identify themselves and enter their own password. To further log-on to the control system software the operations personnel must enter the appropriate code and password. Both of the computers are logged off and shutdown after each transfer or other use.

Operations and Engineering can start up both workstations when required. Engineering may need Operations personnel to perform certain tasks when evaluating the computer controls. Operations personnel control the normal output functions of the system.

2.2.3 INSTRUCTIONS

The Operations personnel are trained to operate the control system by either Engineering personnel or experienced operators. All normal transfer/flush or associated operations shall be performed via operating procedure(s).

Any testing of the cross-site transfer system components shall be performed and controlled by maintenance procedures, functional test procedures, functional checks, or via work package instructions. The type of test (a graded approach to testing) is dependent upon the level of change implemented. The cognizant engineer is responsible for authorizing testing documentation (test plans, etc.).

2.2.4 SOFTWARE STATUS

The software operating on the control system computers shall be monitored by the engineering personnel. The software existing on each of the computers shall be reviewed by the engineering personnel to assure the control system functions properly. Any changes to the computer systems (e.g., addition of memory) shall be documented in the W-058 control System Logbook.

If the current version of the RSI operating system software is being replaced with a later version, the engineering personnel shall perform functional checks to ensure the new version works properly (is compatible with the current computer system hardware and software). All testing by engineering personnel shall be documented in the W-058 Control System Logbook.

2.3 OPERATION AND MAINTENANCE

The control system computers shall be operated by the (SST) operations personnel and maintained by the (SSTE) engineering personnel.

2.3.1 SOFTWARE CUSTODIAN

The individual assigned responsibility for identification, configuration control, distribution, problem notification, and maintenance of the computer programs is the Engineering (SSTE) Manager. As previously stated, the Software Custodian is the Monitor and Control Cog Engineer.

2.3.2 SOFTWARE MAINTENANCE

The RSI software shall be maintained by procuring a yearly maintenance contract with the vendor for their control system software.

The maintenance contract(s) provides updates to the software and operational support, if the software fails or indicates problems. The funding for the maintenance contract(s) shall be provided by Operations (SST) and the Software Custodian shall be identified to the software vendor (RSI) as the POC.

Master copies of the software (the vendor supplied software and the developed ladder logic) shall be installed on the control console and on at least one other engineering (SSTE) workstation. The engineering (SSTE) workstation(s) shall be physically located in another building. The vendor supplied software works on the basis of a key (software) disc system. Hence, only the machine with the software key installed on it can operate the software. Key discs are available from the vendor and expedited delivery can be accomplished, if an immediate need for a second key arises.

Each version or revision of the RSI software is uniquely identified. The associated documentation that defines the changes in the software by each revision shall be obtained and entered into the vendor information (VI) file.

The software master discs shall be maintained by the Software Custodian. The Software Custodian is responsible to identify (in the W-058 Control System Logbook), that the control console software and the backup software (on the engineering [SSTE] workstation[s]) are the same version. The Software Custodian is responsible to install all software on all platforms.

2.3.3 SOFTWARE PROTECTION

The RSI software is protected from vandalization by using password protection. In addition, the 242-S control room is locked unless operations or engineering are working on the control console or software. As previously stated, the access to the computers and software requires knowledge of the system and is password protected.

2.3.4 DATA PROTECTION

The data files associated with the RSI software are located on the control station computers and on at least one engineering (SSTE) workstation.

The data files shall be maintained by the Software Custodian. The Software Custodian is responsible to identify (in the W-058 Control System Logbook) that the control console data files and the backup data files (on the engineering [SSTE] workstation[s]) are the same version. The Software Custodian is responsible to install the data files on all platforms. At the vendor's request, corrupted data files may be forwarded to the vendor to review, if the data file failure could potentially be attributed to the vendor software.

2.3.5 PROTECTION FROM CATASTROPHE

The software program and data files are protected from catastrophe by being located on the control console and at least one engineering (SSTE) workstation. These platforms are located in different buildings and should equipment (computer) failures occur, replacement hardware would be procured at that time.

2.3.6 PROCUREMENT ITEMS

The software program and data files were procured as a part of the W-058 Project. Procurement Specification W-058-P2, "Process Monitor and Control System," defines the contractual agreement that was used to procure the control system and software.

Section 2.3.2, "Software Maintenance," identifies the procurement of a maintenance contract with the software vendor.

2.4 DESIGN LIFE AND DECOMMISSIONING

The life expectancy of the 242-S structure is approximately forty years. The computer control console is built for the current computers. As upgrades occur on the control system hardware, the console may need to be changed. The cabling system and other control components will need to be replaced upon failures and upgraded when the system becomes outdated.

Decommissioning shall occur subsequent to the last transfer being completed and funding has been established for the removal of the equipment.